UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

In the Matter of the Search of

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

9799 Miramar Road
San Diego, California 92126

CASE NUMBER: '08 MJ 1491

I, Matthew W. Chenevey, being duly sworn, depose and say:

I am a Special Agent with the Federal Bureau of Investigation, FBI, and have reason to believe that on the property or premises known as:

9799 Miramar Road
San Diego, California, 92126

[as more fully described in ATTACHMENT A]

in the Southern District of California there is now concealed a certain person or property, namely:
SEE ATTACHMENT B

which is:
(1) property that constitutes evidence of the commission of a criminal offense; and
(2) property designed and intended for use or which is or has been used as a means of committing a criminal offense;

concerning a violation of Title 18, U.S.C., Section1341.
The facts to support a finding of probable cause are as follows:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part thereof.
I specifically request that the judge review this warrant for vagueness and over breath.

Matthew W. Chenevey, Special Agent, FBI

Sworn to before me, and subscribed in my presence
May 12, 2008, at San Diego, California;

CATHY ANN BENCIVENGO, U.S. Magistrate Judge,

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Matthew W. Chenevey, being duly sworn, depose and state that:

EXPERIENCE AND TRAINING

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), United States Department of Justice, and have been so employed since 2004. I am currently assigned to a Counterterrorism Squad of the San Diego Field Office, where my primary assignment is the Investigation of International Terrorism.

2. In addition, I have received extensive training in conducting complex investigations and in the preparation and execution of search warrants while at the FBI Academy in Quantico, Virginia.

3. In preparing this affidavit, I have conferred with other Special Agents and law enforcement officers who have a combined experience of over thirty years in law enforcement, and the opinions stated below are shared by them. Furthermore, I have personal knowledge of the following facts or have been told them by the persons mentioned below.

4. Because this affidavit is being submitted for the limited purpose of seeking authorization to search the premises located at (1) 9799 Miramar Road, San Diego, California, 92126 and (2) 9485 Black Mountain Road, San Diego, California, 92126, I have not set forth each and every fact learned during the course of this investigation, but instead, I have set forth only those facts I believed were necessary to support an order to search the above referenced premises.

PREMISES TO BE SEARCHED

5. There are two premises to be searched: (1) 9799 Miramar Road, San Diego, California; and (2) 9485 Black Mountain Road, San Diego, California. FLAMINGO CAR GROUP is located on premises (1) and (2). FLAMINGO MOTORS INCORPORATED used to do business on premises (2). YOUSEF and IRAN HOODNEH are the owners of FLAMINGO CAR GROUP and YOUSEF HOODNEH owns FLAMINGO MOTORS INCORPORATED.

6. I believe that there is probable cause to search these two premises because I believe that these premises will have United States and foreign monetary instruments, as well as papers, documents, or digital records relating to the purchase or sale of automobiles inside and outside the United States, and that said evidence will establish violations of Title 18 U.S.C. §§ 1341, the crime of mail fraud.

FLAMINGO CAR GROUP

7. According to records of the County of San Diego and the California Board of Equalization ("BOE"), YOUSEF and IRAN HOODNEH are the property owners of FLAMINGO CAR GROUP, which was incorporated on August 6, 2003, and conducts business at Premises 1. The County of San Diego's records indicate that Premises 1 is located on .84 acres of land.

8. Personal inspection by the affiant, as well as the enterprise's own website, establish that FLAMINGO CAR GROUP also conducts business at Premises 2.

FLAMINGO MOTORS INCORPORATED

9. On February 27, 2008, BOE Senior Investigator (SI) Michael Scullion, advised the affiant that YOUSEF HOODNEH is a corporate officer for FLAMINGO MOTORS INCORPORATED, which used to do business at Premises 2.

10. California Secretary of State records show that FLAMINGO MOTORS INCORPORATED has suspended its corporate activities and list the company's address as YOUSEF and IRAN HOODNEH's residence.

11. The affiant has personal knowledge of the location of YOUSEF and IRAN HOODNEH's residence based on the affiant's observations when federal agents arrested YOUSEF HOODNEH at his home on immigration-related offenses.

INVESTIGATION REGARDING VIOLATIONS OF TITLE 18, U.S.C. § 1341

12. BOE audited FLAMINGO MOTORS INCORPORATED's sales tax returns from October 1, 1999, through December 31, 2002. BOE completed the audit on December 23, 2003. Pursuant to the audit, BOE assessed FLAMINGO MOTORS INCORPORATED with $1,931,094.96 worth of unpaid taxes, interest, and penalties.

13. BOE Special Investigator ("SI") Scullion provided the affiant with 2005 sales data for FLAMINGO CAR GROUP. According to SI Scullion, in 2005, FLAMINGO CAR GROUP purchased 610 vehicles from various California automobile auctions and paid $7,701,772.00 for those vehicles. That same year, FLAMINGO CAR GROUP sold $476,700.00 worth of vehicles at auction, resulting in a net purchase via auction of $7,225,072.00 worth of retail inventory.

14. SI Scullion advised the affiant that FLAMINGO CAR GROUP reported its 2005 retail sales to the BOE. For 2005, FLAMINGO CAR GROUP reported total retail sales of $2,925,947.00. Based solely on its 2005 net auction purchases of $7,225,072.00, if FLAMINGO CAR GROUP accurately reported its sales to the BOE, it would have had to hold at least $4,299,125.00 worth of retail inventory at the end of 2005.

15. Investigation by the affiant revealed that it is physically impossible for FLAMINGO CAR GROUP to have held $4,299,125.000 worth of inventory at the end of 2005. As previously discussed, FLAMINGO CAR GROUP has two locations: Premises 1 (9799 Miramar Road, San Diego, California), and Premises 2, (9485 Black Mountain Road, San Diego, California). SI Scullion advised the affiant that car dealers in California are required to license their lots through the BOE. California Department of Motor Vehicles (DMV) Investigator Janis Stidham advised the affiant that California car dealers are also required to license their lots through the DMV. Neither the affiant nor SI Scullion nor Investigator Stidham found any evidence that FLAMINGO CAR GROUP has licensed lots at locations other than Premises 1 and 2.

16. On March 12, 2008, the affiant spoke to MOJGAN MANAVI, also known as MOJGAN BEHROUZI, who was the manager of FLAMINGO CAR GROUP at the end of 2005. She stated that FLAMINGO CAR GROUP only possessed lots at the 9799 Miramar Road and 9485 Black Mountain properties.

17. The affiant obtained aerial photographs of FLAMINGO CAR GROUP's two properties and counted the maximum number of parking spots located on the two properties. The properties hold a maximum of approximately 185 parking spots. The average value of the cars purchased by FLAMINGO CAR GROUP at auction in 2005 was $12,625.00, (which is the 2005 total auction purchases divided by the number of cars bought). Based on the average value of the vehicles purchased by FLAMINGO CAR GROUP in 2005 ($12,625.00) and the total number of cars that it could hold (185), FLAMINGO CAR GROUP could not have held more than $2,335,625.00 worth of vehicles at the end of 2005.

18. SI Scullion advised the affiant that FLAMINGO CAR GROUP sold 100 vehicles at auction in 2005 and that only 6 of the vehicles sold at auction were purchased at auction. As this evidence indicates that FLAMINGO CAR GROUP purchased vehicles at places other than auction, the 2005 auction data does not capture the full value of all the vehicles held by FLAMINGO CAR GROUP during 2005.

19. Nevertheless, assuming that it filled every available parking spot with unsold vehicles at the end of 2005, purchased no cars other than those bought at auction, and placed no commercial mark-up on its retail purchases, FLAMINGO CAR GROUP failed to account for at least $1,963,500.00 in sales for 2005. Based on San Diego County's tax rate of 7.75%, FLAMINGO CAR GROUP failed to pay at least $152,171.25 in sales tax.

20. On May 5, 2008, SI Scullion advised the affiant that FLAMINGO CAR GROUP submitted its 2005 sales tax returns via first class mail through the United States Postal Service. FLAMINGO CAR GROUP submitted four quarterly sales tax returns in 2005, each filed separately through the mail. According to SI Scullion, FLAMINGO CAR GROUP under-reported the sales tax due for retail sales in 2005 and therefore submitted fraudulent sales tax returns to the BOE.

21. Based on my training and experience, consultation with other Agents from the FBI and from other law enforcement agencies, and all of the facts and opinions set forth in this affidavit, I know:

A. It is common for persons and businesses employed in the automobile sales industry to maintain a "jacket" for each vehicle. This "jacket" provides a detailed history for the acquisition and disposition of each vehicle associated with the business.

B. It is common for persons and companies employed in the automobile sales industry to maintain digital records that provide a detailed history for the acquisition and disposition of each vehicle associated with the business.

C. It is common for persons and companies employed in the automobile sales industry to maintain papers, documents, or digital copies of quarterly State sales tax returns and Federal income tax returns.

D. It is common for persons and businesses who file false quarterly sales tax returns to hide the proceeds of their unlawful activity in a secure area on the businesses' premises.

22. Based on my training, experience, and the above-mentioned facts, I believe that probable cause exists that the businesses located at Premises 1 (9799 Miramar Road, San Diego, California, 92126) and Premises 2 (9485 Black Mountain Road, San Diego, California, 92126) maintain United States and foreign monetary instruments, and/or papers, documents, or digital records which evidence the sale of automobiles inside and outside of the United States. The presence of papers, documents, or digital records which evidence the sale of automobiles inside and outside of the United States may indicate, based on my training, experience, and the above-mentioned facts, that YOUSEF HOODNEH, using the businesses located at 9799 Miramar Road, San Diego, California and 92126, 9485 Black Mountain Road, San Diego, California, 92126, has failed to accurately report the amount of sales tax he collected to the State of California's Board of Equalization. This evidence would then also be relevant and necessary to demonstrate a violation of Title 18 U.S.C. §§ 1341, the crime of mail fraud.

DIGITAL EVIDENCE

23. The following information is based upon my knowledge, training, and experience, as well as the knowledge, training and experience of other Agents and computer experts with whom I have consulted, including experts from the San Diego Regional Computer Forensics Laboratory (RCFL).

24. Digital evidence can be stored on a variety of systems and magnetic, optical and mechanical storage devices including, but not limited to, hard disk drives, floppy disks, compact disks, DVDs, magnetic tapes, magneto optical cartridges, personal digital assistants, cellular phones, pagers and memory chips. It can be

created and stored utilizing a variety of different operating systems, applications, utilities, compilers, interpreters and communication programs.

25. Searching and seizing information from computers typically requires agents to seize most or all electronic storage devices, along with related peripherals, to be imaged and searched later by a qualified computer expert in a laboratory or other controlled environment. This is because searching computer systems is a highly technical process and because computer storage devices can store the equivalent of thousands of pages of information.

26. Technical Requirements: Searching computers and computer systems is a highly technical process that requires specific expertise, equipment and software. It is best conducted in a controlled environment such as the RCFL.

A. The vast array of hardware and software available today makes it difficult to know before a search which expert is qualified to conduct the examination and which equipment is needed to conduct the examination. In some cases, the CFE may need to train with particular software and/or obtain additional hardware before a proper examination can be accomplished.

B. Data search protocols are exacting scientific procedures designed to safeguard the integrity of a computer forensic examination and to locate and recover hidden, erased, compressed, password-protected and encrypted files. An important part of the protocol is the creation of a complete, forensically sound image of the original digital evidence before an examination of the evidence is conducted. There are numerous pitfalls, including inadequate power supply, unusual computer system architecture, and conflicts with specific software or file systems that can seriously hamper the possibility and integrity of an imaging process conducted on-site, rather than in a controlled environment.

C. Another reason that it is sometimes impracticable to conduct an on-site image is that some operating systems, such as Linux, Unix, MAC and Novell, are "hardware" specific, which means that a restored image of original digital evidence may not be "bootable" or "viewable" without the actual original hardware. This would prevent the CFE from viewing the restored digital image in a manner consistent with the structure of the original digital evidence.

D. Additional problems are created by the growing use of destructive programs or "booby traps." These programs can destroy or alter data if certain forensic procedures are not scrupulously followed. Since digital evidence is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment is essential to conducting a complete and accurate examination of any digital evidence.

E. Finally, there is a growing use of data security and encryption programs by consumers. The encryption programs, which are inexpensive and widely available, allow users to encrypt specific data with just a few keystrokes. Newer technologies, like steganography, which allows a user to conceal information within other files, create additional difficulties in conducting forensic examinations. A controlled environment is necessary to obtain an accurate image of the digital evidence and to conduct an appropriate search.

27. The Volume of Evidence: The volume of data stored on a typical computer system is so large that it is unrealistic to search for specific data while conducting an on-site examination.

A. Computer storage devices, such as hard disks, tapes, diskettes, compact disks and DVDs, can store the equivalent of millions of pages of information. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives capable of storing more than 60 gigabytes of data are commonplace in new desktop computers. It may take days to weeks to examine a computer, depending on the amount of data and whether the user has taken efforts to hide, delete or encrypt the data.

B. A complete forensic search, however, is not limited to examining files normally displayed by the operating system. It also includes the expansion of compressed data and the recovery of deleted file data. It involves the areas on a computer hard drive that the computer system recognizes as being "in use" and those areas that the computer system deems "available for use." This search may involve an examination of "slack" space, which is the information at the end of a sector or cluster beyond the end of the "current" usage. Finally, the complete examination would address "orphaned" data, portions of files left behind by earlier operating system activity. All of these areas require operating specific tools and techniques to access the data, which are best accomplished on a computer image in a controlled environment.

C. It is very easy for a computer user to conceal data or other types of digital evidence through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension "jpg" are digital image files. A moderately sophisticated computer user, however, can easily change the .jpg file extension to "txt" or "dll" in order to conceal or mislead law enforcement into thinking the digital image is actually a text or system file. While it may be possible for a CFE to notice this during a properly controlled forensic examination, it is difficult for that same CFE to do detect this concealment during an on-site examination.

28. For the reasons noted above, it is not appropriate to conduct any type of "partial" image, without first creating a forensically sound full and complete image of the original digital evidence. Data can be spread throughout many portions of the original digital evidence and may be lost if a CFE attempted to just "copy all images" or download "any E-mail."

SEARCH METHOD

29. Based upon the investigation conducted so far, I expect to find several computers. Every effort will be made to "image" any computer systems found "on-site." I also know that it is not always possible to conduct a proper forensic image of a computer system on site. The following factors, if present, may require the RCFL to seize a computer system in order to conduct a forensic image at the RCFL:

A. Hardware Compatibility Problems: There are many different types of computers manufactured today, many of which use proprietary hardware and software during the creation of any user data. It is impractical for the law enforcement community to have all the proper adapters, cables, cords and other hardware devices necessary to consistently link law enforcement forensic equipment with all known and unknown computer systems on an immediate basis while imaging "on-site." Much of this specialized equipment is available, but may need to be acquired in order to conduct a proper forensic image

B. Software Compatibility Problems: There are occasions when the specialized software used by CFEs to conduct a forensic image in the field does not work correctly. This may be caused by a number of reasons, including unusual target system architecture or conflicts with specific software or file systems installed on the targeted system.

C. Sufficient On-Site Power Accommodations: To make a forensically sound image of digital evidence found on-site, the CFE must ensure that there is an adequate uninterruptible power supply. Digital evidence is extremely fragile and susceptible to power interruptions and power surges. The location of the site or the number of computers on the site may make it difficult to provide sufficient uninterruptible power supplies during the forensic imaging process.

D. The Need To Have Access To Original Equipment: It may be necessary for the CFE to have access to the original digital evidence during the course and scope of the forensic examination due to the type of hardware and software being utilized.

E. Complexity Of The System Architecture: More sophisticated computer users may be able to create "proprietary" computer networks that the CFE

may be unfamiliar with. This is generally noticeable during the execution of the search warrant. Moreover, if the computer user or system administrator is uncooperative in providing the relevant details of the computer system and any unfamiliar computer system architecture discovered during the execution of the search warrant, then it may be necessary to seize and examine the systems, prior to imaging, in a safe and controlled environment.

30. There may be other factors that arise on-site that cannot be foreseen at the time of the preparation of this search warrant application. If, in the opinion of the CFE, there are technical difficulties, such as noted above or otherwise arising at the time of the search, the CFE shall have the ability to forego on-site imaging and to seize any digital media for transport to either a secure Evidence Storage Facility or the RCFL for proper forensic imaging and examination.

31. In the event that any computer systems or digital media is seized and transported to the RCFL, the seized item will be imaged within 30 days and the original evidence will be returned.

32. Searching the seized computers and digital evidence for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a "keyword" search that searches through the files stored in a computer for special words that are likely to appear only in the materials covered by a warrant. Similarly, agents may be able to locate the materials covered in the warrant by looking for particular directory or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete or hide files to evade detection; or take other steps designed to frustrate law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as locating and examining deleted information, examining disk space not allocated to listed files, or opening and reviewing every file. I, therefore, request permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

BACKGROUND ON COMPUTERS

33. The term "computer" as used herein is defined as set forth in 18 U.S.C. § 1030(e)(1), and includes any electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

34. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

A. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, other commercial entities and universities. To access the Internet, an individual computer user must subscribe to an Internet Service Provider or ISP, which operates a host computer system with direct access to the Internet. In the work environment, many governmental entities, corporations and universities provided employees and students with access to the Internet

B. A device known as a modem allows any computer to communicate with another computer through the use of telephone lines or cable. The modem may be internal or external to the computer.

C. By connection to the Internet, either through a commercial ISP or through access provided by a private service provider such as the government, an individual with a computer can make electronic contact with millions of computers around the world.

35. Based on training and through my personal use of computers, I have knowledge of the method by which e-mail and other files are transmitted over telephone lines or cable between computers. Based on my training and knowledge I know the following:

With the modem, a computer user can transport a computer file to his own computer, so that the computer file is stored in his computer. The process of transporting a file to one's own computer from another is called "downloading."

The user can then view the file on his/her computer screen (monitor), and can "save" or retain the file on his/her computer for an indefinite time period.

In addition to permanently storing the file on the computer, the user may print the file.

The original file that is downloaded is also maintained in the originating computer.

With the modem, a computer user can send a file from the computer to another individual on the Internet. This process of sending a file is called "uploading.

The process of "uploading" is similar to the "downloading" process except the user is sending the computer file to others instead of retrieving the information from another computer. As with the process of "downloading," the original file is maintained on the originating computer.

A user can also use an e-mail program to send files to another individual on the Internet. Most e-mail programs allow the user to attach files to the e-mail. The attached files may be documents or images. Again, the original file is maintained on the originating computer.

CONCLUSION

Based on the foregoing, I believe there is probable cause to support the issuance of a search warrant for the businesses located at Premises 1 (9799 Miramar Road, San Diego, California, 92126) and Premises 2 (9485 Black Mountain Road, San Diego, California, 92126) and furthermore that there is probable cause that these premises contain evidence of violations of Title 18 U.S.C. § 1341– mail fraud.

The statements in this affidavit are made based on my personal observations and the investigation conducted by your affiant, as well as information communicated or reported to your affiant during the investigation by other participants in the investigation, as the content of this affidavit indicates.

Further affiant sayeth not.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

MATTHEW W. CHENEVEY
Special Agent, Federal Bureau of Investigation

Sworn to before me and subscribed in my presence, in San Diego, California, on May 12, 2008.

Honorable Cathy Ann Bencivengo
United States Magistrate Judge

ATTACHMENT A

PREMISES TO BE SEARCHED

A single story building at 9799 Miramar Road, San Diego, California, 92126, which is located on the Southwest corner of Kearny Mesa Road and Miramar Road in San Diego, California, is accessed through two gates: one each located adjacent to Southbound Kearny Mesa Road and Eastbound Miramar Road.

The single story building at 9799 Miramar Road, San Diego, California, 92126, which is sand colored, has the red letters "FLAMINGO CAR GROUP Inc." affixed to the roof. The main structure is marked with the number "9799" on the Northeast side of the building, just above the single door. Motion activated, double doors are located to the left of the single door on the Northeast side of the building.

Two small trailers are located in the rear of the main structure at 9799 Miramar Road, San Diego, California, 92126. The Northwestern-most trailer is light brown in color with two windows. A white sign with black letters "Modular Building Concepts, Inc. (858)679-1185" is hanging between the two windows. The door to this trailer is white in color, and it is raised on a yellow platform. The Northwestern-least trailer is light brown in color with two windows. A dark brown door is between the two windows. A yellow sign with the red letters "FLAMINGO CAR RENTAL & LEASING" is to the left of the door. This trailer is also raised on a yellow platform.

ATTACHMENT B

ITEMS TO BE SEIZED

The items to be seized are evidence of violations of Title 18, United States Code, Section 1341, specifically:

A. Any and all computer software and hardware including, but not limited to, hard drives, diskettes, zip diskettes, compact diskettes, Secure Digital cards, Compact Flash cards, Memory Sticks, Micro Secure Digital cards, and DVDs, which may contain stored information relating to the acquisition and/or disposition of automobiles, the collection of State of California sales tax, the proceeds of mail fraud, mail fraud, business income tax returns (Federal and State), or State of California sales tax returns.

B. Any and all documents evidencing the acquisition and/or disposition of automobiles.

C. Any and all documents evidencing the collection of State of California sales tax.

D. Any financial records which may contain information relating to the acquisition and/or disposition of automobiles, collection or payment of sales tax, or the proceeds of mail fraud.

E. Any financial records associated with the State of California's Board of Equalization and correspondence between Flamingo Car Group, Flamingo Motors, Yousef Hoodneh, or Iran Hoodneh, and the State of California's Board of Equalization.

F. Copies of business income tax returns, Federal and State, including Forms 1099 and any other records used in the preparation of income tax returns.

G. Copies of State of California sales tax returns for Flamingo Car Group, Inc., and Flamingo Motors, Inc., including any documents or other records used in the preparation of sales tax returns.

H. Cash, checkbooks, bank statements, cancelled checks, and miscellaneous correspondence.